UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/224,918	01/04/1999	HEATH HUNNICUTT	1001/028C	3147

22801 7590 10/16/2002

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER
EDELMAN, BRADLEY E

ART UNIT	PAPER NUMBER
2153	18

DATE MAILED: 10/16/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 18

Application Number: 09/224,918
Filing Date: January 04, 1999
Appellant(s): HUNNICUTT ET AL.

Bradley Desandro
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on August 26, 2002.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The grouping of the claims is correct.

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

U.S. Patent No. 5,235,642 (Wobber et al.), issued August 10, 1993.

U.S. Patent No. 5,506,961 (Carlson et al.), issued April 9, 1996.

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

1. Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

In considering these claims, all of the independent claims – 1, 15, 31, 35, 37, 39, 41, 42, 44, 46, 47, and 49 – include limitations that were not described in the specification at the time the application was filed. The specification describes two separate processes. One process involves access requests received from users. When a user makes a request to access a resource, the system determines whether the user may obtain access to the resource by checking an access cache. See Specification, p. 16-18; Fig. 5. The other, separate, process involves flushing the cache if particular access rights or resources have changed. On a regular, periodic basis, the system will check if certain access rights, resources, or access lists have changed, and if they have, the access cache will be flushed of all related access permissions from the

cache. See Specification, p. 18-19; Fig. 6. These two processes operate on some of the same data, but they are separate processes that occur independently of each other.

Each of the independent claims essentially combines these two separate steps into a single, if-then-else routine stemming from a single access request. For instance, claim 37 describes that a server first receives a request for a resource, then checks a memory to determine whether certain parameters have changed, then, if the parameters have changed, the cache memory relating to the user and resource is flushed, but if the parameters have not changed, the system goes on to determine whether a similar request has been previously granted and grants access if the determination is affirmative. However, as explicitly stated in the specification, the steps of checking for alterations and flushing the cache occur on a *regular, periodic basis*. These steps occur separately from any access requests, and there is no routine described in the specification that combines these two separate features. As stated above, one process receives access requests and responds accordingly, while the other process periodically checks for resource or access rights alterations and responds to that determination accordingly. On step does not occur as a result of the other, as claimed.

Therefore, because the claims include new matter that was not described in the specification at the time the application was filed, these claims must be canceled from the application, or appropriately corrected.

2. Claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In considering claims 1, 3-5, 7-11, 14-15, 17-25, and 28-36, and 41, the independent claims – 1, 15, 31, 35, and 41 – all include language that is indefinite. All of these claims include if-then-else statements that do not logically flow from the preceding claim language. For instance, claims 1 recites the following:

"Checking a first memory . . . to determine:

if [one of three criteria is met], then removing any access permissions from the first memory . . .

else, if the first memory indicates that the user has previously accessed the resource, then providing the user with access to the requested resource."

The step of "determining" should not include within it steps of removing or providing access to a user. Perhaps the result of the determination step would be to provide access, but these claims, as presently worded, actually include the removing and providing steps as part of the determination step. Therefore, claims 1, 15, 31, 35, and 41, and all claims depending therefrom must be canceled from the application or appropriately corrected. Note: as an example of language that is not indefinite in this respect, see claim 39.

In considering claims 37-40, 42-49, the independent claims – 37, 39, 42, 44, 46, 47, and 49 – include language that is unclear. Each of these claims requires a step of

checking if "the user is/was logically present." It is unclear as to how an actual user can be logically present in a cache. Perhaps the claims intended to mean checking if a *representation* of the user is/was present in the cache, as recited in claims 1, 15, 31, and other independent claims. Nonetheless, claims 37, 39, 42, 44, 46, 47, and 49, and all claims depending therefrom, as presently stated are unclear, and must be canceled from the application or appropriately corrected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49, as understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over Wobber et al. (U.S. Patent No. 5,235,642, hereinafter "Wobber").

For the purposes of these claims, Examiner has interpreted the claims as including the two separate functions of (1) authenticating users who have or have not previously accessed the resources, and (2) flushing the cache of access permissions if particular system settings are altered.

In considering claims 1, 15, and 31, Wobber discloses a system for a computer-implemented method, comprising:

means for checking a first memory (local cache 164) to determine if a user has previously accessed a requested resource on a computer network without performing a file open procedure upon a file which are stored any access permissions of users for access to the resource (col. 7, lines 32-36), upon receipt of an indication from the user to access the resource (col. 7, lines 22-24); and

providing the user with access to the resource if the first memory indicates that the user has previously accessed the resource (col. 8, lines 31-35).

See also, the Abstract and Summary of the invention.

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or when access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no

longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claims 3 and 17, Wobber further discloses that the user is represented in the first memory by a token (Auth ID, col. 7, lines 34-38).

In considering claims 7 and 21, Wobber further discloses that the resource is a file (col. 4, line 21).

In considering claims 8 and 22, Wobber further discloses that the resource is a volume of files (col. 4, line 21).

In considering claims 9 and 23, Wobber fails to explicitly disclose that the resource is a memory device (see col. 4, lines 21-24). However, Examiner takes official notice that it is well known for networking systems to control access to memory devices, as well as for software objects. Thus, it would have been obvious to a person having ordinary skill in the art to use the access control system taught by Wobber for networked memory devices in order to speed up the authorization process for access requests made to such memory devices.

In considering claims 10 and 24, although the system taught by Wobber discloses substantial features of the claimed invention, it fails to explicitly disclose storing of the information in the first memory comprising overwriting other information associated with the resource in the first memory. Nonetheless, Examiner takes official notice that it is well known in a network resource access system that authentication information is often changed and can thus be overwritten. One reason to change authentication information is to prevent tampering of the protected resources. Therefore, given the likelihood of tampering, it would have been obvious to a person having ordinary skill in the art to overwrite the token (Auth ID) taught by Wobber with a new token submitted from the user to help prevent security breaches.

In considering claims 11 and 25, although the system taught by Wobber discloses substantial features of the claimed invention, it fails to disclose writing a token for the user in the first memory over another token for another user that had last previous access to the resource. Nonetheless, Examiner takes official notice that overwriting information related to access rights in a network system is well known. Examiner takes further official notice that overwriting of data in a cache according to a least-recently-used algorithm is well known. Thus, given these well known network access functions, it would have been obvious to a person having ordinary skill in the art to include the step of overwriting the least-recently-used tokens in the token cache in the system taught by Wobber, in order to open up storage space in the token cache in case the memory has become full.

In considering claims 14 and 28, Wobber further discloses the request from the user indicating an operation to perform with respect to the resource (i.e. access the resource), and further comprising:

checking the first memory (local cache 164) to determine if the user may perform the operation with respect to the resource (col. 7, lines 34-36);

checking a second memory (local cache 160) to determine if the user may perform the operation with respect to the resource if the first memory does not indicate that the user may perform the operation with respect to the resource (col. 7, lines 39-40, 44-45, 48-52);

providing the user with access to the resource if the second memory indicates that the user may perform the operation with respect to the resource (col. 7, lines 50-60); and

storing information in the first memory indicating that the user may perform the operation with respect to the resource if, after checking the second memory, the second memory indicates that the user may perform the operation with respect to the resource (col. 7, lines 58-63).

In considering claim 20, Wobber further discloses authorizing the user by checking a password (Auth ID) provided by the user; associating the token (Principal ID) with the user after authorizing the user; and using the token to check the first memory (col. 8, lines 1-30; col. 7, lines 55-62).

In considering claims 29 and 30, Wobber further discloses:

checking a second memory to determine if the user may access the resource if the first memory does not indicate that the user has previously accessed the resource (col. 7, lines 39-40, 44-45, 48-52);

providing the user with access to the resource if the second memory indicates that the user may access the requested resource (col. 7, lines 50-60); and

storing information in the first memory indicating that the user may access the resource if, after checking the second memory, the second memory indicates that the user may access the requested resource (col. 7, lines 58-63).

In considering claim 32, Wobber further discloses performing a file open procedure upon the file in which are stored any access permissions of users for access to the requested resource to determine if the requesting user may access the requested resource if the memory does not indicate that the requesting user has previously accessed the requested resource (col. 7, line 64 – col. 8, line 22); and

providing the requesting user with access to the requested resource if the requested resource indicates that the requesting user may access the requested resource (col. 8, lines 23-30).

In considering claim 33, Wobber further discloses storing information in the memory indicating that the user has previously accessed the requested resource (col. 8, lines 22-30).

In considering claim 34, Wobber further discloses prior to checking the memory, performing a preliminary memory check to determine of the requesting use has previously accessed the computer network (col. 4, lines 37-65).

In considering claim 35, Wobber further discloses a machine-readable program storage device embodying instructions executable by a computer to perform a method for providing access to a plurality of resources to a plurality of requesting users wherein access to each said resource is controlled by a network server having a network memory, the method comprising:

receiving at the network server a resource request to access a requested resource of said plurality of resources from one said requesting user (col. 4, lines 9-30), wherein:

the network memory has stored therein which of said plurality of requesting users had accessed which of said plurality of resources (col. 7, lines 34-36); and

an access file has stored therein any access permissions of any users for access to the requested resource (col. 7, line 64 – col. 8, line 22);

without opening the access file, checking the network memory to determine if the requesting user had accessed the requested resource (col. 7, lines 34-36); and

if the requesting user had accessed the requested resource, opening the requested resource to provide access to the requesting user (col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or when access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 36, Wobber further discloses when the requesting user had not previously accessed the requested resource:

opening the access file; checking the access file to determine if the requesting user may have access to the requested resource; and if the check is affirmative, then providing said access (col. 7, line 64 – col. 8, line 22).

In considering claim 37, Wobber discloses a resource access system comprising:

a network, including a plurality of resources, for transmitting a resource request from a network user with access to the network for access to a requested resource of said plurality of resources (col. 4, lines 9-30); and

a network server (node 102-1), in communication with the network, for:

receiving the resource request (col. 7, lines 22-24);

checking, without opening any of said plurality of resources, whether the network user's resource request had been previously granted (col. 7, lines 34-36); and

granting said access if the check is affirmative (col. 8, lines 31-34).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6,

lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or when access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 38, Wobber further discloses that granting said access further comprises opening the requested resource for the network user to have said access to the requested resource (col. 8, lines 34-35).

In considering claim 39, Wobber discloses a program for a resource access system, the program being embodied on a computer-readable medium and executed on a server that provides access to resources on a network, the program comprising: a code segment to receive a resource request for access to one said resource from a user having access to the network (col. 7, lines 22-24);

a code segment to check, without opening any of said resources on the network, whether the user had previously been granted access to the requested resource (col. 7, lines 34-36; and

a code segment to grant said access if the check is affirmative (col. 8, lines 31-35).

However, Wobber does not explicitly disclose code segments for determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or when access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 40, Wobber further discloses a code segment to open the requested resource for the user of the network to have said access to the requested resource if the check is affirmative (col. 8, lines 34-35).

In considering claim 41, Wobber discloses a method for controlling access to a requested resource on a computer network by a requesting user, the method comprising:

checking a first memory, without opening the requested resource, to determine if the requesting user has previously accessed the network (col. 7, lines 34-36); and

if the requesting user has previously accessed the network:

providing the requesting user with access to the network (col. 8, lines 31-35);

checking a second memory, without opening the requested resource, to determine if the requesting user has previously accessed the requested resource (col. 7, lines 48-52);

if the requesting user has previously accessed the requested resource then providing the requesting user with access to the requested resource (col. 7, lines 52-63); and

if the requesting user has not previously accessed the requested resource then opening the requested resource to determine if the requesting user may access the requested resource and if the requested resource indicates that the requesting user

may access the requested resource then providing the requesting user with access to the requested resource (col. 7, line 64 – col. 8, line 22).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the second memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or when access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 42, Wobber further discloses a resource access determination method comprising: receiving a request for an access to a resource from

a user having had said access; and deciding the request affirmatively based upon contents stored in a cache without opening the resource or contacting the user (col. 7, lines 22-24, 30-38; col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or if access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 43, Wobber further discloses, prior to said receiving: receiving a request for an access to the resource from the user who had not previously accessed the resource; and obtaining any access privileges to the resource of the user without contacting the user (col. 7, line 64 – col. 8, line 22; col. 8, lines 38-44).

In considering claim 44, Wobber discloses a resource access determination method comprising:

receiving an initial request for an access to a resource from a user, and obtaining an access privilege of the user to the resource from a cache and without contacting the user (col. 7, line 64 – col. 8, line 22; col. 8, lines 38-44); and

if the user had the access privilege to the resource: granting the initial request; receiving subsequent requests for subsequent accesses to the resource from the user; and granting each said subsequent request without: opening the resource; or contacting the user (col. 7, lines 22-38; col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or if access permissions have

changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 45, Wobber further discloses that granting the initial request further comprises caching the result of said obtaining said access privilege of the user to the resource (col. 8, lines 23-30); and

granting each said subsequent request further comprises comparing each said subsequent request with said cached result of said obtaining said access privilege of the user to the resource (col. 7, lines 34-48).

In considering claim 46, Wobber discloses a resource access determination method comprising: receiving a request for an access to a resource from a user having had said access; and deciding the request affirmatively based upon contents stored in a cache prior to contacting the user and without opening the resource (col. 7, lines 22-38; col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or if access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 47, Wobber discloses in a system where resources are protected by access checks that are performed to confirm that a user meets any requirements for access to a particular resource, and where an access check is performed the first time that the user requests access to the particular resource to confirm that the user meets any requirements for access to the particular resource, a

method for determining whether the user should have access to the particular resource (col. 4, lines 9-30; col. 8, lines 1-22), the method comprising:

receiving a request from a user for access to a resource; checking the results of previous access request checks, which results are stored in a memory cache, to determine if the user has previously been allowed access to the resource; if the user has previously been allowed access to the resource, then allowing access to the resource without performing an access check (col. 7, lines 22-38; col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or if access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a

person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

In considering claim 48, Wobber further discloses that the results of previous access request checks are cached in a cache (col. 8, lines 23-30).

In considering claim 49, Wobber discloses in a system where resources are protected by access checks that are performed to confirm that a user meets any requirements for access to a particular resource, where the requirements for each user to access each resource are stored in an access file, where an access check is performed the first time that the user requests access to the particular resource to confirm that the user meets any requirements for access to the particular resource, and where the access check that is performed the first time that the user requests access to the particular resource includes performing a file opening procedure upon the access file to determine the requirements for the user to access the particular resource (col. 7, line 64 – col. 8, line 22), a method for determining whether the user should have access to the particular resource, the method comprising:

receiving a request from a user for access to a resource (col. 7, lines 22-24);

checking the results of previous access request checks, which results are stored in a memory cache, without opening the access file, to determine if the user has previously been allowed access to the resource (col. 7, lines 34-36); and

if the user has previously been allowed access to the resource, then allowing access to the resource without performing an access check (col. 8, lines 31-35).

However, Wobber does not explicitly disclose the steps of determining if (1) the requested resource is altered, or (2) a representation of the user has been removed from the first memory, or (3) any of the access permissions of the user for access to the requested resource are altered; and if any one of those three criteria is satisfied, then removing the relevant access permissions from the memory. Instead, Wobber proposes a time stamp for removing validity of the access rights from the cache (col. 6, lines 21-22). Nonetheless, Examiner takes official notice that removing user access rights to a network resource when the resource is altered, or if access permissions have changed is notoriously well known in the art. A person having ordinary skill in the art would have readily recognized the desirability and advantages of removing access permissions to the resources taught by Wobber not only when the time stamp expires, but also when the resources are altered or access rights have changed, in case the altered resources include classified information which should not be viewed by current users, or the current users have been demoted from classified status and should no longer have access to classified information. Thus, it would have been obvious to a person having ordinary skill in the art to remove user access rights to the resources taught by Wobber when resources or access permissions are altered.

4. Claims 4, 5, 18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wobber, in view of Carlson et al. (U.S. Patent No. 5,506,961,

hereinafter "Carlson").

In considering claims 4, 5, 18, and 19, although the system taught by Wobber discloses substantial features of the claimed invention, it fails to disclose that the token also represents anonymous users and/or a plurality of other users. Nonetheless, it is well known for multiple users of a networked system to maintain the same tokens (thus remaining anonymous) for user access to a resource, as evidenced by Carlson. In a similar art, Carlson teaches an access rights system that uses tokens to signify access rights of users to a network, wherein single tokens can identify a group of users (thus rendering the users anonymous; col. 8, line 63 – col. 9, line 5). Thus, given the teaching of Carlson, a person having ordinary skill in the art would have readily recognized the desirability of representing multiple users with the same anonymous token to decrease the number of entries and amount of data in the cache, thus speeding up the cache look-up time. Therefore, it would have been obvious to represent a plurality of users in the system taught by Wobber with the same token, as suggested by Carlson.

(11) Response to Argument

Applicant has traversed all claim rejections made in the final rejection sent on March 27, 2002. These claim rejections were made in response to amendments to the claims that changed the scope of the claims and thus necessitated all of the new grounds of rejection set forth in the final rejection.

Applicant has appealed five separate grounds of rejection. Each of these grounds will now be addressed in turn.

I. The 35 U.S.C. 112, first paragraph claim rejections, directed toward pending claims 1, 3-5, 7-11, 14-15, 17-25, and 28-49.

All pending claims are rejected under 35 U.S.C. 112, first paragraph because all of the independent claims include limitations that were not described in the specification at the time the application was filed. As described in the Final Rejection, the specification describes two independent processes of the invention: one process determines whether a user may obtain access to a resource by accessing an access cache (see p. 16-18, Fig. 5); and the other process describes flushing the cache if particular access rights or resources have changed (see p. 18-19, Fig. 6). The amended independent claims, however, include language that attempts to fuse *both* processes into a conditional if-then-else process. Such a combination is nowhere disclosed in the specification. Applicant has failed to point to a location in the specification where this function is disclosed. Instead, Applicant has argued that the amended claim language is supported in the original *claims* of the *parent* application (Application No. 08/689,838, now U.S. Patent No. 5,889,952), relying on MPEP 608.01(l). Examiner is not persuaded by this argument for two reasons.

First, MPEP 608.01(l) does not state that an applicant may rely on the claims of a *parent* application in establishing a disclosure of a present application. Instead, MPEP 608.01(l) merely states, "In establishing a disclosure, applicant may rely not only on the

description and drawing as filed but also on the original claims if their content justifies it." Thus, because § 608.01(l) of the MPEP makes no mention of reliance on parent applications, Applicant has improperly relied on this section of the MPEP in attempting to establish disclosure of the presently claimed invention.

Second, even if Applicant's reliance on the claims of the parent application were proper, those claims still do not disclose the presently claimed invention. The original parent claims relied upon by Applicant include independent claim 1, and dependent claims 18-22 (see p. 7-8 of Appeal Brief). In relying on these claims, Applicant argues, "The FIRST PROCESS *recited in Claim 1* generates an 'access permission' that is stored in an 'access cache.' The SECOND PROCESS *recited in claims 18-22* performs 'tracking security changes' upon 'said access-cache' with respect to 'said access-permissions' . . . [t]hus the SECOND PROCESS . . . is inherently preceded by the FIRST PROCESS." (Italics added). This language is entirely different from the "if X, then Y, else Z" language used in the present claims. The language of the parent claims, as evidenced by the structure of the parent claims and as supported by Applicant's argument in the Appeal Brief, *at best*, discloses a sequential order of the processes.[1] However, the conditional language appearing in the present claims requires more than simply one process occurring before another process. It requires a conditional if-then-else process. Therefore, because the conditional function stated in the presently claimed invention is not supported anywhere in either the present

[1] Examiner respectfully disagrees that the claim language necessitates the first process (providing access to two specific users of a resource claimed in claim 1) inherently preceding the second process (updating the cache claimed in dependent claims 18-22). The dependent claims make no mention of any *specific*

application or the parent application, the 35 U.S.C. 112, first paragraph rejections are proper.

Regarding Applicant's argument with respect to the SECOND PROCESS alone, Examiner agrees that the second process of removing access permissions when a resource, user, or access permission changes is disclosed in the specification, and thus Examiner withdraws any assertions to the contrary.

II. The 35 U.S.C. 112, second paragraph claim rejections, directed toward pending claims 1, 3-5, 7-11, 14-15, 17-25, 28-36, and 41.

Regarding these claims, Examiner believes the language used in independent claims 1, 15, 31, 35, and 41 is ambiguous because the if-then-else statements are unclear and do not logically flow from the preceding claim language. Applicant argues that the language is clear, stating that the logical function of "'determining if X, then Y, else Z,' where Z can include further 'if/then' logic strings" is a well understood concept and convention in the art. Examiner respectfully disagrees. The claim language, when read in its grammatical context, essentially states, "Determine if X: Then do Y; Determine else if Z: Then do R." The step of 'determining else if Z' does not make grammatical sense. Alternatively, the statement can read, "Determine if X, then [regardless of the determination] do Y, else if Z [unclear whether 'else' refers to X or Y], then do R." Thus, the claim language is open to various confusing interpretations and it

---

user, resource, or access-permission described in claim 1. Thus, the updating process may occur at any

does not follow conventional if-then-else language. It is unclear whether the claimed invention performs the typical if-then-else computer programming process, or whether it performs a different process. Examiner mentioned in the final rejection that claim 39 of the present application provides an example of language that is not indefinite regarding conditional processes. However, claims 1, 15, 31, 35, and 41 were not stated in a similar way to claim 39, so for the reasons stated above, the 35 U.S.C. 112, second paragraph rejections are proper.

III. The 35 U.S.C. 112, second paragraph claim rejections, directed toward pending claims 37-40, and 42-49.

Examiner rejected these claims because they include the limitation of checking if "the user is/was logically present or removed." Examiner asserted that it is unclear how an actual *user* can be logically present in a cache. Applicant traversed this rejection, stating that "the plain meaning of the recited limitation 'logically' is readily understood, both with respect to when a 'network user is logically removed' as recited in claims 37-40, and with respect to when 'the user was logically present' as recited in claims 42-49." Examiner respectfully disagrees that use of the terminology that "users" may be "logically present" is conventional and readily understood in the art. Users, as understood in the art, are people who use a particular system. The use of the term "logical presence" in concordance with human beings is not a conventional practice in the art. Granted, determining whether a particular electronic state or specific data

---

time, before *or* after a particular user accesses the system.

associated with a user is logically present in a computer is an understandable, if not conventional, term of art. But, determining whether a human being is logically present is both unclear and unconventional in the computer arts. Examiner cannot imagine any logical manner in which an actual human being can be placed into a computer cache. Examiner mentioned in the final rejection that claims 1, 15, and 31 provide an example of language that is not unclear regarding logical presence. However, claims 37-40 and 42-49 were not stated in a similar way as claims 1, 15, and 31, so for the reasons stated above, the 35 U.S.C. 112, second paragraph rejections are proper.

IV. The 35 U.S.C. 103(a) claim rejections, directed toward pending claims 1, 3, 7-11, 14, 15, 17, 20-25, and 28-49.

The issue regarding these claims is whether Applicant seasonably traversed Examiner's statements of Official Notice. Examiner maintains that Applicant failed to seasonably traverse the official notice such that the official notice statements are now taken to be admitted prior art, pursuant to 37 CFR 1.111(b) and MPEP 2144.03.

A brief review of the prosecution history is in order. Applicant has provided a detailed description of the prosecution history of the case on pages 14-17 of the Appeal Brief. In addition, the most pertinent facts are described below:

1. A non-final rejection was mailed to Applicant on August 1, 2001. In the rejection, all independent claims were rejected under 35 U.S.C. 102(b) as being anticipated by

Wobber et al. (U.S. Patent No. 5,235,642), and certain dependent claims were rejected under 35 U.S.C. 103(a), wherein Examiner took Official Notice that the features described in these claims were well known in the art.[2]

2. In response to the non-final rejection, Applicant first amended the claims to incorporate the subject matter of the "Official Notice" dependent claims into the independent claims, and then Applicant disputed Examiner's taking of Official Notice. Applicant's argument stated the following:

> Applicants respectfully submit that the rejection fails to give proper weight to these limitations, especially since these limitations are missing from the prior art of record. Moreover, these assertions of obviousness are not otherwise supported by way of prior art citation, stated scientific theory, basis for common knowledge in the art, or cited legal precedent. . . Due to such absence of support for the limitations now present in the amended independent claims, the Applicants respectfully submit that the obviousness rejections are to be withdrawn as to the claims now pending. The applicant respectfully submits that, as to the claims now pending, a *prima facie* case of obvious (sic) has not been made out, or in the alternative, the pending claims avoid the rejections.

Paper 14 at 24-25. In this response, Applicant did not demand a reference regarding the information asserted as well-known by Examiner, and Applicant additionally failed to assert that the information regarded as well-known in the Official Notice statements was in fact not well known.

---

[2] These Official Notice statements are as follows: "It is well known for networking systems to control access to memory devices"; "it is well known in a network resource access system that authentication information is often changed and can thus be overwritten"; "overwriting information related to access rights in a network system is well known"; "removing user access rights to a network resource when the resource is altered is well known"; and "altering user access privileges to a resource in a network is well known." Examiner later provided examples of systems that employ these functions, such as a corporate server deleting access rights to employees who are fired, group printer access rights being deleted when a particular printer is removed from the system, and access rights being overwritten when a user's security clearance changes. See Paper 15 at 21, 26-27.

3. In response to Applicants amendments, which altered the structure and scope of the claims, a final rejection was mailed to Applicant. Because the features of the previous dependent claims were thereby incorporated into the independent claims, Examiner rejected the amended independent claims under 35 U.S.C. 103(a), taking Official Notice to the same features that were noted in the non-final rejection as being well-known. Examiner further noted that Applicant's attempted traversal of the Official Notice statements was not seasonable, because it failed to both demand a reference supporting the asserted facts, and to state why the noticed facts are not considered to be well known in the art. See Paper 15 at 26-27. As a result, and pursuant to MPEP 2144.03, Examiner took Applicant's failure to adequately traverse the Official Notice statements as an admission that the noted features were well-known in the art.

4. Applicant submitted the Appeal Brief, arguing primarily that Examiner has not given proper weight to the limitations missing from Wobber et al., and demanding either evidence or an explanation to be given as to why the demanded evidence is not required. Applicant *again* failed to rebut the Official Notice statements regarding the well-known features.

This brings us to the present.

The MPEP states the following:

> If applicant does not seasonably traverse the well known statements during examination, then the object of the well known statement is taken to be admitted prior art. *In re Chevenard,* 139 F.2d 71, 60 USPQ 239 (CCPA 1943). A seasonable challenge constitutes a demand for evidence

> made as soon as practicable during prosecution. Thus, applicant is charged with rebutting the well known statement in the next reply after the Office action in which the well known statement was made.

MPEP § 2144.03. From the history described above, it is clear that Applicant did not demand evidence as soon as practicable during prosecution (i.e. in the response to the non-final rejection). Furthermore, it is also clear that Applicant did not rebut the well known statements in the next reply after the Office action in which the well known statement was made (i.e. in the response to the non-final rejection). In fact, even after a *second* opportunity to rebut the well known statements (i.e. the Appeal Brief), Applicant still failed to do so. Applicant's only argument is that the official notice statements lacked sufficient evidentiary weight to support the claim features. In other words, Applicant complained that Examiner did not support the Official Notice statements with evidence, and thus Examiner improperly rejected the claims. However, such evidence is not necessary when Official Notice is taken – that is the very essence of Official Notice. Evidence is only required when Applicant seasonably traverses Examiner's statements of Official Notice. Applicant has not done so here, and thus the object of the well known statement is taken to be admitted prior art, as required by MPEP § 2144.03. Therefore, for the reasons stated above, the 35 U.S.C. 103(a) rejections are proper.

V. The 35 U.S.C. 103(a) claim rejections, directed toward pending claims 37-40 and 42-49.

Claims 37-40 and 42-49 were rejected under 35 U.S.C. 103(a) as being unpatentable over Wobber et al., in view of Carlson et al. (U.S. Patent No. 5,506,961).

Applicant's arguments regarding these claims do not address the application of the Carlson et al. reference, but only rely on the Official Notice portion of the claims already discussed above. Therefore no further discussion regarding these claims is necessary.

For the above reasons, it is believed that all rejections should be sustained.

Respectfully submitted,

Bradley Edelman
October 11, 2002

Conferees

Dung C. Dinh
Primary Examiner

ZARNI MAUNG
PRIMARY EXAMINER

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201